

WHAT IS CLAIMED IS:

1 1. A method for evaluating transactions for suspicious activity, the
2 method comprising:

3 providing a reference designator list, wherein the reference designator list
4 includes at least a subset of information available from a first transaction system that is
5 associated with suspicious activity;

6 evaluating a first transaction associated with the first transaction system using
7 the reference designator list to detect suspicious activity; and

8 evaluating a second transaction associated with a second transaction system
9 using the reference designator list to detect suspicious activity.

10 2. The method of claim 1, wherein the subset of information is a first
11 subset of information, the method further comprising:

12 receiving a second subset of information from the first transaction system; and
13 incorporating the second subset of information into the reference designator
14 list.

15 3. The method of claim 2, the method further comprising:

16 receiving a third subset of information from the second transaction system;
17 and

18 incorporating the third subset of information into the reference designator list.

19 4. The method of claim 2, wherein the incorporating the second subset of
20 information into the reference designator list comprises:

21 creating a new reference designator;

22 associating the second subset of information with the new reference
23 designator; and

24 adding the new reference designator to the reference designator list.

25 5. The method of claim 3, wherein the second subset of information
26 comprises a telephone number.

27 6. The method of claim 3, wherein the second subset of information
28 comprises a credit card number.

1 7. The method of claim 3, wherein the second subset of information
2 comprises a name.

1 8. The method of claim 3, wherein the second subset of information
2 comprises an address.

1 9. The method of claim 1, wherein the first transaction system is a system
2 for analyzing authorization requests, and wherein the authorization request is received via a
3 telephone call.

1 10. The method of claim 1, wherein the first transaction system:
2 receives an authorization request at a receiving center, wherein the
3 authorization request is associated with a request to charge a credit account;
4 determining an origin of the authorization request; and
5 comparing the origin of the authorization request with the information point in
6 the reference designator list.

1 11. The method of claim 1, wherein the first transaction system:
2 receives an authorization request at a receiving center, wherein the
3 authorization request is associated with a request to charge a credit account;
4 determining an origin of the authorization request;
5 investigating the origin of the authorization request, wherein it is determined
6 that the authorization request is suspicious; and
7 providing the origin of the authorization, wherein the origin of the
8 authorization comprises at least a portion of the subset of information and is incorporated into
9 the reference designator list.

1 12. The method of claim 11, wherein the origin of the authorization
2 request is a telephone number associated with a location from which the authorization request
3 is initiated.

1 13. A method for detecting fraudulent authorization requests, the method
2 comprising:
3 receiving an authorization request at a receiving center, wherein the
4 authorization request is associated with a request to charge a credit account;

5 determining an origin of the authorization request; and
6 comparing the origin of the authorization request to one or more data
7 associated with suspicious activity.

1 14. The method of claim 13, wherein the origin of the authorization
2 request is a telephone number.

1 15. The method of claim 14, wherein the one or more data associated with
2 suspicious activity are included in a reference designator list.

1 16. The method of claim 13, wherein the one or more data associated with
2 suspicious activity are included in a reference designator list, and wherein at least one of the
3 one or more data was received from a fraud detection system implementing a method selected
4 from the group consisting of:

5 a method for detecting suspicious money transfers; and
6 a method for detecting suspicious credit card activity.

1 17. A system for evaluating transaction for suspicious behavior, the system
2 comprising:
3 a first transaction system; and
4 a second transaction system, wherein both the first and the second transaction
5 systems are in communication with a fraud detection system.

1 18. The system of claim 17, wherein the fraud detection system compiles
2 suspicious information from the first transaction system and suspicious information from the
3 second transaction system into a reference designator list available to both the first and
4 second systems.

1 19. The system of claim 18, wherein the first transaction system
2 comprises:
3 a receiving center adapted to receive an authorization request to charge a
4 credit account; and
5 a fraud investigation system coupled to the receiving center, wherein the fraud
6 investigation system is configured to determine if the authorization request is suspicious.

1 20. The system of claim 19, wherein the second transaction system
2 comprises:
3 a money transfer system.